Method for securing of executable programs against utilisation by an unauthorized person and security system for its application.

Patent number:	DE69326497T
Publication date:	2000-02-10
Inventor:	STASI CORINNE (FR)
Applicant:	GEMPLUS CARD INT (FR)
Classification:	
- international:	G06F12/14
- european:	
Application number:	DE19936026497T 19930427
Priority number(s):	FR19920005187 19920427

Also published as:

EP0568438 (A1)
FR2690540 (A1)
EP0568438 (B1)

Abstract not available for DE69326497T
Abstract of correspondent: **EP0568438**

The invention relates to a method for securing an executable program and especially the program for connection to a workstation. The method consists in hiding a key in a random-data area, locking execution of the program, the deciphering of the address of this key being possible only by authorised persons.
Application to security protection of a workstation.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) Übersetzung der europäischen Patentschrift

(97) EP 0 568 438 B1

(10) DE 693 26 497 T 2

(51) Int. Cl.[7]: G 06 F 12/14

(21) Deutsches Aktenzeichen: 693 26 497.7
(86) Europäisches Aktenzeichen: 93 401 084.4
(96) Europäischer Anmeldetag: 27. 4. 1993
(97) Erstveröffentlichung durch das EPA: 3. 11. 1993
(97) Veröffentlichungstag der Patenterteilung beim EPA: 22. 9. 1999
(47) Veröffentlichungstag im Patentblatt: 10. 2. 2000

(30) Unionspriorität:
9205187 27. 04. 1992 FR

(73) Patentinhaber:
Gemplus Card International, Gemenos, FR

(74) Vertreter:
Beetz und Kollegen, 80538 München

(84) Benannte Vertragstaaten:
DE, ES, FR, GB, IT

(72) Erfinder:
Stasi, Corinne, Cabinet BALLOT-SCHMIT, F-75116 Paris, FR

(54) Verfahren zum Sichern von ausführbaren Programmen gegen die Benutzung durch eine unbefugte Person und Sicherheitssystem für seine Anwendung

DE 693 26 497 T 2

DE 693 26 497 T 2

Die Erfindung betrifft ein Programm zur Sicherung von ausführbaren Programmen gegen die Benutzung durch eine unbefugte Person.

Die Erfindung betrifft alle durch Datenverarbeitungsvorrichtungen ausführbaren Programme. Sie betrifft insbesondere Programme, die die Herstellung einer Verbindung mit einem Informatiksystem ermöglichen, wie dies zum Beispiel mit dem Betriebssystem DOS und noch mehr mit dem Betriebssystem UNIX der Fall ist, das allgemein in den Arbeitsplätzen verwendet wird. Es wird daran erinnert, daß man unter Arbeitsplatz einzelne zugeordnete Geräte großer Rechenkapazität versteht, die Anwendungen wie z.B. CAO ermöglichen und im allgemeinen mit dem Betriebssystem arbeiten.

Es ist nämlich üblich, daß die Verbindung mit einem Arbeitsplatz über ein ausführbares UNIX-Verbindungsprogramm hergestellt wird.

Das erfindungsgemäße Verfahren wird vorteilhafterweise für die Sicherung solcher Verbindungsprogramme verwendet.

Es wird weiter daran erinnert, daß bei Arbeitsplätzen das Verbindungsprogramm ausgeführt wird, um einen Dialog zu initialisieren. Hierzu gibt ein Benutzer über die Tastatur einen ihm eigenen Benutzernamen und ein Paßwort ein, das ihm zugeteilt wurde. Die Paßwörter und die Benutzernamen der Personen, die berechtigt sind, sich zu verbinden, sind dem System bekannt. Wenn es eine Übereinstimmung zwischen den vorher gespeicherten und den über die Tastatur eingegebenen Informationen gibt, wird das Verbindungsprogramm ausgeführt und die Verbindung wird hergestellt.

D1: GB-A-2 205 667 (NCR Corporation) betrifft ein Kontrollverfahren eines Sicherheitsmoduls, das insbesondere zur Über-

prüfung persönlicher Identifikationscodes (PIN) oder zur Zugriffskontrolle anwendbar ist. Bei der Initialisierung wird eine beliebige Zahl KSK in einem Register gespeichert - das auf Null zurückgestellt werden kann, wenn ein Einbruch festgestellt wird -. Dann wird ein Zugriffsberechtigungsschlüssel KA an den Modul angewendet, der mittels KSK verschlüsselt wird, z.B. indem eine DES-Verschlüsselung an das Paar KSK-KA angewendet und in einen geschützten Speicher 36 geladen wird. Schließlich wird das ursprüngliche Programmpaket in den Programmspeicher geladen.

Vor jedem Laden eines veränderten Programmpakets wird ein entsprechender Zugriffsberechtigungswert FAV berechnet und gleichzeitig in den Speicher geladen. Ein im Modul befindlicher Prozessor berechnet den Zugriffsberechtigungswert FAV' neu mittels des gespeicherten Zugriffsberechtigungsschlüssels KA. Der so erhaltene Wert FAV' wird mit dem Wert FAV verglichen, um die Ladung des veränderten Programmpakets zu berechtigen.

EP-A-0 339 115 (Siemens) beschreibt ein Schutzverfahren für ein Programm, gemäß dem ein erster Datensatz (D1), der von Merkmalen des Systems (M1) und dem Programm zugeteilten Attributdaten (A1, A2) gebildet wird, codiert wird, um einen zweiten Datensatz zu bilden, der es ermöglicht, die Anwendung des Programms freizugeben.

US-A-4 944 008 (PIOSENKA et al.) betrifft ein elektronisches Datensperrsystem, das die Daten in Abhängigkeit von einem variablen Schlüssel verändert, der mit Hilfe einer pseudozufälligen Zahl und einer Schlüsselvariablen erhalten wird.

Es hat sich aber herausgestellt, daß solche Schutzvorrichtungen nicht unfehlbar ist, da es zu häufig vorkommt, daß unberechtigte Personen die Verbindungen herstellen können.

Die vorliegende Erfindung ermöglicht die Lösung dieser Aufgabe.

Sie hat ein Sicherungsverfahren für ein beliebiges mit Datenverarbeitungsvorrichtungen ausführbares Programm und insbesondere ein Sicherungsverfahren für das Programm zur Verbindung mit einem Arbeitsplatz zum Gegenstand.

Die vorliegende Erfindung hat insbesondere ein Verfahren zur Sicherung eines durch Datenverarbeitungsvorrichtungen ausführbaren Programms gegen jede Benutzung durch eine unberechtigte Person zum Gegenstand.

Das Verfahren ist im Anspruch 1 definiert.

Ein entsprechendes System ist im Anspruch 7 definiert.

Weitere Merkmale und Vorteile der Erfindung gehen aus der detaillierten Beschreibung hervor, die nur beispielhaft und nicht einschränkend zu verstehen ist. Diese Beschreibung bezieht sich auf die beiliegenden Zeichnungen, in denen:

Figur 1 ein allgemeines Schema der erfindungsgemäßen Sicherungseinheit darstellt;

Figur 2 ein Organisationsschema eines erfindungsgemäßen Programmspeichers darstellt;

Figur 3 eine Tabelle zeigt, die die Austauschvorgänge zwischen einer Chipkarte und Verarbeitungsvorrichtungen darstellt.

Figur 1 zeigt Verarbeitungsvorrichtungen 1, die in Form eines mit einer Tastatur 2 verbundenen Mikrocomputers oder Arbeitsplatzes dargestellt sind. Natürlich können diese Verabeitungsvorrichtungen ein beliebiges anderes Informatiksystem sein, das ein Programm zur Sicherung gegen unbefugte Benut-

zungen ausführen kann. Zur Vereinfachung wird nachfolgend von System gesprochen.

Der Programmspeicher wird durch einen Bereich mit dem Bezugszeichen 3 symbolisch dargestellt und ist in Figur 2 detaillierter gezeigt.

In diesem Programmspeicher 3 sind ein oder mehrere Programme gespeichert. Die Ausführung mindestens eines dieser Programme ist so gesperrt, daß es nur von berechtigten Personen gestartet werden kann. Hierzu enthält das ausführbare Programm P einen in einem Bereich ZA zufälliger Daten versteckten Schlüssel, genannt Hauptschlüssel, der nur von einer berechtigten Person entschlüsselt werden kann.

Der Hauptschlüssel ist ein zufälliger Datenwert, der vom berechtigten Benutzer zum Zeitpunkt der Installierung des Programms in das System eingegeben wird und der an einer Adresse in diesem Bereich ZA versteckt ist, die durch Verschlüsselung erhalten wird. Die Adresse wird ausgehend vom Hauptschlüssel und einem für das Programm eindeutigen Datenwert verschlüsselt.

Die Verschlüsselung der Adresse besteht zum Beispiel darin, einen Algorithmus DES (oder RSA) an den vom Hauptschlüssel und vom für das Programm eindeutigen Datenwert gebildeten Datenwert anzulegen.

Gemäß einem bevorzugten Ausführungsbeispiel besteht der für das Programm eindeutige Datenwert aus dem Datum der Installierung des Programms in das System, Datum, das vom System gegeben wird und das nur für dieses Programm gilt, da es die Stunde, die Minuten und die Sekunden berücksichtigt, und da die Wahrscheinlichkeit, das gleiche Datum zu erhalten, praktisch Null ist.

Gemäß einem bevorzugten Ausführungsbeispiel ist außerdem der Schlüssel im Bereich ZA in zufälliger Weise aufgesplittert.

Der Schlüssel enthält n Bytes. Jedes Byte ist in diesem Bereich an einer Adresse verteilt, die daher auch aufgesplittert ist. Die Adresse jedes Bytes entspricht einem Byte des Ergebnisses der Verschlüsselungsrechnung. Man kann sich auf das Schema der Figur 2 beziehen, in dem als Beispiel die Standorte AD von acht Bytes eines Hauptschlüssels mit acht Bytes im Bereich ZA dargestellt sind.

Der eindeutige Datenwert, das heißt das Installierungsdatum, ist an einer dem System bekannten, aufgesplitterten, aber festen Adresse im Bereich ZA gespeichert, so daß das System den Hauptschlüssel zum gegebenen Zeitpunkt wiederfinden kann.

Wenn in einem System ein Programm auf diese Weise gesichert ist, haben die berechtigten Benutzer über den Austausch geheimer Informationen die Möglichkeit, die Ausführung dieses Programms in der nachfolgend beschriebenen Weise freizugeben.

So besitzt praktischerweise jeder Benutzer eine Speicherkarte, auf der ein nur dem Karteninhaber bekannter Geheimcode, ein dem Karteninhaber ebenfalls bekannter Benutzername und ein geheimer Referenzschlüssel gespeichert sind.

Wenn eine berechtigte Person die Ausführung des gesicherten Programms starten möchte, führt diese Person ihre Karte 22 in das Lesegerät 20 ein, das mit dem System 1 verbunden ist, und dann gibt er über die Tastatur 2 des Systems seinen Geheimcode und seinen Benutzernamen ein. Dann werden über das Lesegerät Austauschvorgänge zwischen dem System und der Karte durchgeführt. Diese Austauschvorgänge sind in der Tabelle der Figur 3 dargestellt, und sie sollen die Entschlüsselung des Hauptschlüssels durch eine beliebige berechtigte Person durchführen, die folglich zugriffsberechtigt und befugt ist.

18.10.99

Der Hauptschlüssel (CL.M.) ist wie oben beschrieben im Bereich ZA versteckt.

Das System berechnet den Referenzschlüssel CL.REF ausgehend von CL.M. und der auf der Karte gelesenen Seriennummer.

$$CL.REF = f(CL.M, \text{Seriennummer})$$

Die Funktion f wird vorzugsweise für alle Verschlüsselungsrechnungen durch einen Algorithmus der Art DES oder RSA durchgeführt.

Nach dieser ersten Berechnung schickt das System einen ersten zufälligen Datenwert Alea 1 an die Karte.

Die Karte errechnet ein Verschlüsselungsergebnis Rc ausgehend von Alea 1 und CL.REF.

Das System errechnet seinerseits ein Ergebnis Rs, derart, daß:

$$Rs = f(CL.REF, \text{Alea } 1)$$

Das System empfängt von der Karte einen zweiten zufälligen Datenwert Alea 2 und das Ergebnis Rc.

Das System vergleicht Rs und Rc. Wenn diese Ergebnisse gleich sind, wird die Karte zugriffsberechtigt, sonst wird sie zurückgewiesen. Anschließend nimmt man Rs = Rc = R.

Das System errechnet dann einen Dialogschlüssel S.

$$S = f(R, \text{Alea } 2)$$

Das System schickt dann einen verschlüsselten Datenwert Data an die Karte, so daß:

18.10.99

Data = f^{-1} (S, Code.Sec), wobei f^{-1} der Kehrwert von f ist.

Die Karte errechnet dann ein Ergebnis Rd, so daß:

$$Rd = f(Data, S)$$

Die Karte vergleicht die gespeicherten Datenwerte Rd und Code.Sec, um zu wissen, ob der vom Benutzer eingegebene Code mit dem auf der Karte identisch ist.

Wenn dies der Fall ist, wird der Benutzer zugriffsberechtigt. Es gibt in der Tat eine gegenseitige Zugriffsberechtigung zwischen dem System und dem Karteninhaber.

Das System errechnet dann ein Ergebnis Rn derart, daß:

$$Rn = f(NOM, S)$$

Der Datenwert NOM ist der auf der Karte gespeicherte Benutzername.

Das Ergebnis Rn wird zum System übertragen, das den Datenwert NOM entschlüsselt, indem es die Funktion f^{-1} (Kehrwert von f) anwendet.

$$f^{-1} (Rn, S) = NOM$$

Wenn der entschlüsselte Datenwert NOM gleich dem vom Benutzer eingegebenen Datenwert NOM ist, ist dieser Benutzer befugt.

Wenn die Zugriffsberechtigung stattgefunden hat, wird das Programm ausgeführt.

Bei der Installierung des so geschützten Programms verfügt der Monteur über eine Installierungskarte, die es ermöglicht, den Hauptschlüssel zu speichern, den der berechtigte Benutzer über die Tastatur in das System eingegeben hat und der im Be-

reich ZA gespeichert ist, und den Referenzschlüssel ausgehend von diesem Hauptschlüssel und der Seriennummer der Karte zu berechnen, die dem Benutzer übergeben wird. Die Installierungskarte wird verwendet, um die Benutzerkarten zu erstellen. Diese Installierungskarte wird nämlich verwendet, um die Identifikationsinformationen der Karte und ihres Inhabers zu speichern, d.h.: der Geheimcode, der Benutzername, der Referenzschlüssel.

Wie oben gesagt, wird das Programm insbesondere für Arbeitsplätze angewendet. Es ermöglicht zum Beispiel in diesem Fall, den Zugriffsmodus zum Arbeitsplatz zu sichern, wobei das gesicherte ausführbare Programm dann das Verbindungsprogramm ist.

Das Verfahren kann auch im Fall eines gemieteten Programms verwendet werden, um eine Kontrolle der Anzahl von Benutzungen des Programms durch einfaches Zählen der Zugriffe auf dieses Programm durchzuführen und den Zugriff und somit die Ausführung zu sperren, wenn die Anzahl von Benutzungen einen vorher eingegebenen Grenzwert überschritten hat, der vom Mietvertrag vorgesehen wurde.

Ansprüche

1. Verfahren zur Sicherung eines Programms (P), das durch Datenverarbeitungsvorrichtungen (1) ausführbar ist, gegen jede Verwendung durch unberechtigte Personen, dadurch gekennzeichnet, daß es die folgenden Schritte umfaßt:

   A) zum Zeitpunkt der Installierung des Programmes
   - Auswahl und Einführung eines Hauptschlüssels (CL.M) durch einen berechtigten Benutzer zum Sperren der Ausführung des Programmes,
   - Berechnen einer Speicheradresse des Hauptschlüssels innerhalb eines Blocks (Z.A) von im ausführbaren Programm enthaltenen Zufallsdaten durch Verschlüsselung, wobei die Berechnung der Speicheradresse des Hauptschlüssels darin besteht, diesen Hauptschlüssel mit einem für das Programm eindeutigen Datenwert mittels eines Verschlüsselungsalgorithmus (DES) zu verschlüsseln, wobei das Ergebnis n Bytes aufweist,
   - Speichern dieses Hauptschlüssels an dieser Adresse,

   B) während der Benutzungen
   - Entschlüsseln der Adresse des Hauptschlüssels aus Identifikationsinformationen und/oder Zugriffsberechtigungsinformationen der Person, die die Ausführung des Programms starten will, wobei die Identifikation und/oder Zugriffsberechtigung besteht in:
     Ausgabe einer Chipkarte an jeden berechtigten Benutzer, auf der vorher Identifikations- und/oder Zugriffsberechtigungsinformationen der Karte und des Inhabers gespeichert wurden, wobei diese Informationen umfassen:
     - die Seriennummer der Karte,
     - einen Identifikationsnamen des Karteninhabers,

- einen dem Inhaber bekannten Geheimcode,
- einen Referenzschlüssel (CL.REF), der von dem Hauptschlüssel abhängt,
- Identifikation und/oder Zugriffsberechtigung der Person, wenn die Entschlüsselung zum Start der Ausführung des Programms erfolgreich durchgeführt wurde, wobei die Karte den Geheimcode, der durch die Person eingegeben wurde, mit einem berechneten Datenwert vergleicht.

2. Sicherungsverfahren nach Anspruch 1, bei dem der Hauptschlüssel ein Zufallsdatenwert mit n Bytes ist, der zufällig durch das ausführbare Programm ausgewählt wird.

3. Sicherungsverfahren nach einem der vorhergehenden Ansprüche, bei dem der Hauptschlüssel im Block von Zufallsdaten in mehrere Adressen aufgesplittert ist.

4. Verfahren nach dem vorhergehenden Anspruch, bei dem der Schlüssel derart aufgesplittert ist, daß jedes Byte sich an der Adresse befindet, die durch jedes Byte von n Adressenbytes gegeben ist, die durch Verschlüsselung erhalten wurden.

5. Verfahren nach einem der vorhergehenden Ansprüche, bei dem der eindeutige Datenwert jedes Programms dessen Installationsdatum in die Verarbeitungsvorrichtungen ist.

6. Verfahren nach einem der vorhergehenden Ansprüche, bei dem der Schritt der Identifikation und/oder Zugriffsberechtigung darin besteht, eine gegenseitige Zugriffsberechtigung zwischen der Karte und dem System herzustellen, und für die Karte besteht in:
   - Übertragen der Seriennummer der Karte an die Verarbeitungsvorrichtungen,
   - Berechnen eines ersten Ergebnisses durch Verschlüsseln des residenten Referenzschlüssels und eines ersten empfangenen Zufallswerts,

- Berechnen eines zweiten Ergebnisses (S) durch Verschlüsseln des vorhergehenden Ergebnisses und eines zweiten Zufallswerts, und Übertragen des ersten Ergebnisses und des zweiten Zufallswerts,
- Berechnen des Geheimcodes durch Verschlüsseln ausgehend von einem empfangenen Datensatz (Data) und dem zweiten Ergebnis,
- Vergleichen des durch die Berechnung erhaltenen Geheimcodes mit dem residenten Geheimcode,
- Zugriffsberechtigung des Benutzers, wenn die beiden Codes identisch sind,
- Übertragen des Namens des Karteninhabers in verschlüsselter Form,

und für die Verarbeitungsvorrichtungen besteht in:

- Berechnen des Referenzschlüssels durch Verschlüsseln der Seriennummer ausgehend vom Hauptschlüssel,
- Übertragen eines ersten Zufallswerts,
- Berechnen eines Ergebnisses durch Verschlüsseln des ersten Zufallswerts und des erhaltenen Referenzschlüssels,
- Vergleichen dieses Ergebnisses mit dem ersten auf der Karte erhaltenen Ergebnis,
- Berechnen eines Dialogschlüssels durch Verschlüsseln des Ergebnisses und des zweiten Zufallswerts,
- Berechnen eines Datenwertes (Data) durch Entschlüsseln des Dialogschlüssels und des vom Benutzer eingegebenen Geheimcodes,
- Übertragen dieses Datenwertes (Data) auf die Karte,
- Entschlüsseln des von der Karte empfangenen Namens und Vergleich mit dem eingegebenen Namen.

7. Gesichertes Informatiksystem mit Datenverarbeitungsvorrichtungen (1) mit einem Programmspeicher, in welchem ein oder mehrere ausführbare Programme gespeichert sind, wobei die Vorrichtungen mit einer Tastatur und einem Kartenlesegerät verbunden sind, dadurch gekennzeichnet, daß der Programmspeicher einen Bereich umfaßt, in dem mindestens ein ausführbares Programm (P) gesichert ist, dessen

Ausführung nur bei Berechtigung stattfinden kann, das Programm dafür einen Hauptschlüssel (CL.M) enthält, der vom berechtigten Benutzer zum Zeitpunkt der Installation des Programms ausgewählt und eingegeben und an einer verschlüsselten Adresse innerhalb eines Blocks (Z.A) von Zufallsdaten in dem Bereich gespeichert wird, in dem das Programm gespeichert ist, wobei die Berechnung der Speicheradresse des Hauptschlüssels darin besteht, diesen Hauptschlüssel mit einem für das Programm eindeutigen Datenwert mittels eines Verschlüsselungsalgorithmus zu verschlüsseln, wobei das Ergebnis n Bytes aufweist, und daß die Karten der berechtigten Benutzer außer der Seriennummer der Karte einen Identifikationsnamen des Karteninhabers, einen dem Inhaber bekannten Geheimcode und einen Referenzschlüssel (CL.REF) enthalten, der vom Hauptschlüssel abhängt, wodurch es den Verarbeitungsvorrichtungen ermöglicht wird, die Adresse des Hauptschlüssels zu entschlüsseln und den Karteninhaber zu identifizieren und/oder zugriffsberechtigt zu machen und so die Ausführung des Programms freizugeben, wenn der Inhaber seinen Geheimcode und seinen Benutzernamen eingegeben und die Karte den Geheimcode, der durch die Person eingegeben wurde, mit einem berechneten Datenwert verglichen hat.

8. Informatiksystem nach Anspruch 7, dadurch gekennzeichnet, daß die Verarbeitungsvorrichtungen einen Arbeitsplatz enthalten.

FIG_1

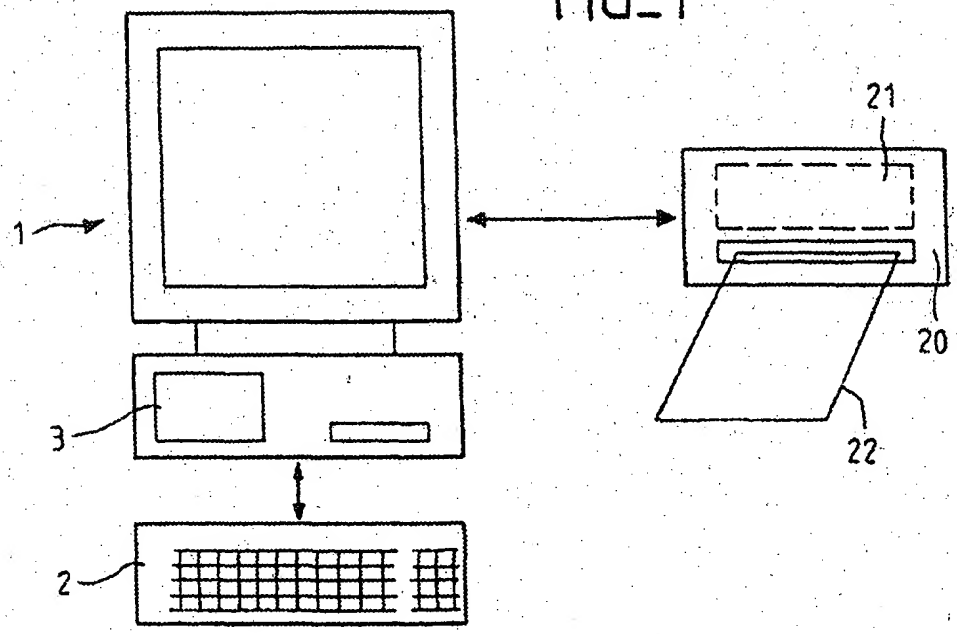


FIG_2

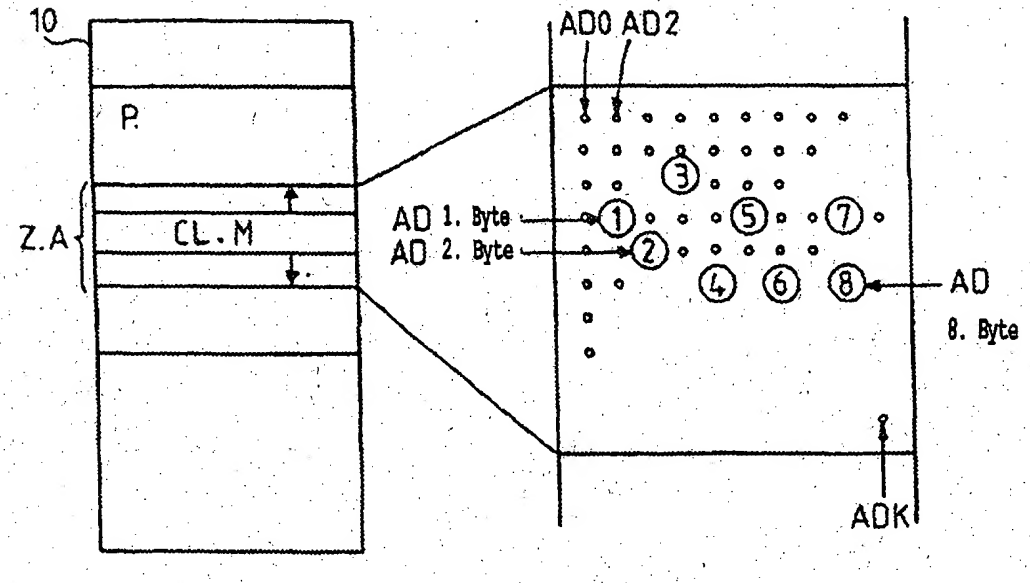
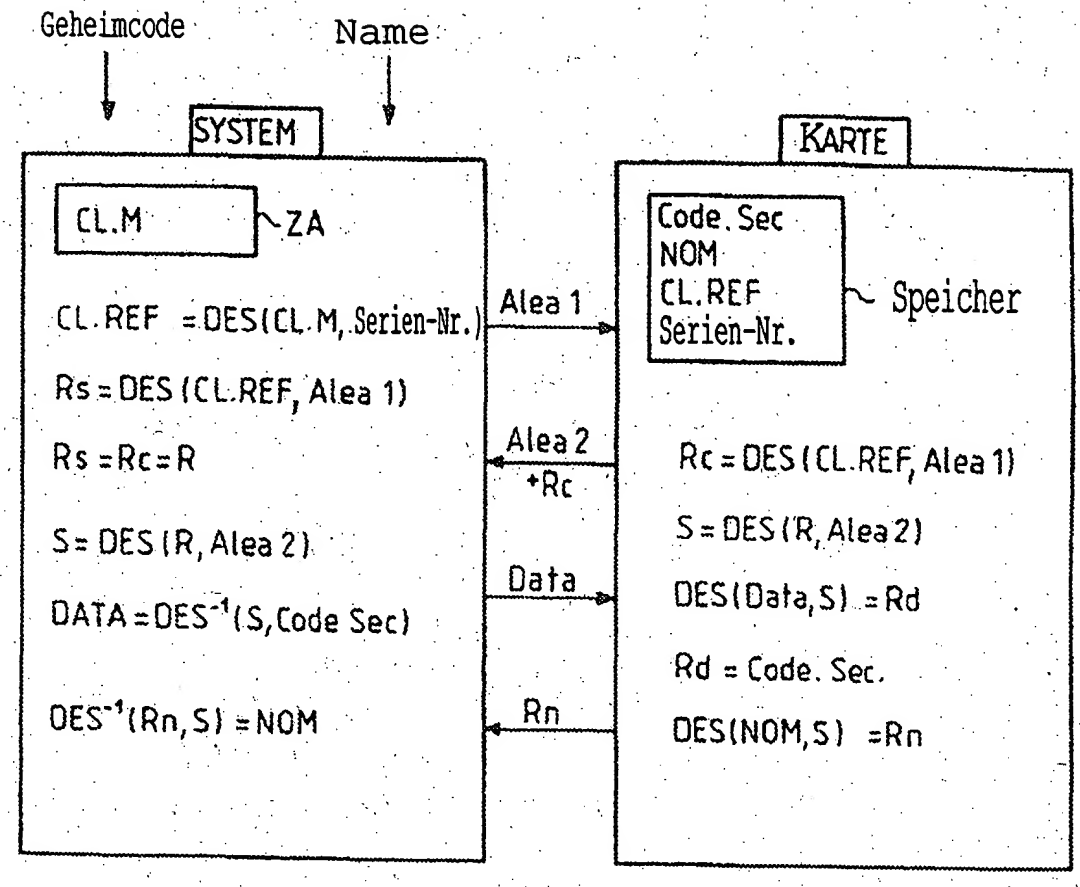


FIG_3


Geheimcode
Name
SYSTEM
CL.M
ZA
CL.REF = DES(CL.M, Serien-Nr.)
Rs = DES (CL.REF, Alea 1)
Rs = Rc = R
S = DES (R, Alea 2)
DATA = DES⁻¹(S, Code Sec)
DES⁻¹(Rn, S) = NOM
KARTE
Code. Sec
NOM
CL.REF
Serien-Nr.
Speicher
Alea 1
Alea 2
+Rc
Data
Rn
Rc = DES (CL.REF, Alea 1)
S = DES (R, Alea 2)
DES(Data, S) = Rd
Rd = Code. Sec.
DES(NOM, S) = Rn